

Safeguarding Customer Information

July 1, 2011

PURPOSE

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003.

The purpose of establishing an identity theft prevention program is to detect, prevent and mitigate identity theft by identifying and detecting identity theft "red flags" and responding in a manner that will prevent identity theft.

Definitions

Covered Account - An account that the creditor offers or maintains for which there is a reasonable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Credit - Is the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment?

Creditor - Is any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continues credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Identifying Information - Is any name or number that can be used alone or in conjunction with other information. Identifying information includes name, address, phone number, social security number, driver license, and birth date, and birth certificate, certificate of naturalization, permanent resident card, credit report, background report, medical records, and education records.

Identity Theft - Means fraud committed or attempted using the identifying information of another person without authority.

Red Flag - A "red flag" indicates a pattern or practice associated with the possibility of identity theft.

Policies and Procedures

- Identify "red flags" and incorporate them into our program.
- Detect "red flags" that have been incorporated into our program.
- Respond appropriately to "red flags" that have been detected.

Safeguarding Customer Information

July 1, 2011

- Update the program periodically to reflect changes in risks to potential identity theft.

Identification of "Red Flags"

The following "red flags" have been identified:

- A fraud, active duty alert, or credit freeze on a credit report
- Notification of an address discrepancy
- A pattern of credit activity that is inconsistent with the usual pattern
- Documents that appear to be forged or altered
- Photographs or physical descriptions that are not consistent with the appearance of the individual
- Information on documentation that is inconsistent with the information supplied by the individual
- An application or document that appears to have been forged, or gives the appearance of having been destroyed and reassembled
- Name, birth date, place of birth, and social security number inconsistencies
- Non-existent (bogus) addresses and phone numbers
- Information such as social security number, address, or phone is similar to information on another account
- Information provided on required forms is incomplete, vague, or inconsistent with previously known information
- Inability to answer questions beyond information provided from a "wallet"
- Any unusual or inconsistent activity on an account
- Notification from an outside source, creditor, or law enforcement agency

Detection of "Red Flags"

In order to detect "red flags", the institution will take the following steps:

- Require multiple forms of identification such as name, address, phone number, driver license, and social security card be presented for comparison.
- Request correlating information associated with, but not represented on any documentation
- Verify the identity of individuals who call or email requesting vital information
- Verify changes in address, phone, or account information

Response to Suspected Identity Theft

If a "red flag" has been detected, the following steps will be implemented. The steps utilized will depend on the degree of risk posed by the "red flag."

Safeguarding Customer Information

July 1, 2011

- Continue to monitor or research evidence of identity theft
- Contact the individual at risk
- Alter any password or other security devices that permit access to an individual's information
- Notify the Program Administrator to determine the appropriate steps to take.
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances
- Discontinue all activity or interaction until a decision has been reached

In order to prevent the likelihood of identity theft occurring with respect to the internal operating procedures at the institution, the following steps will assure the protection of student's identifying information.

- Ensure the security of our website, office computers, laptops, and cell phones
- Ensure complete and secure destruction of paper documents containing student information
- Keep offices clear of papers containing student information
- Keep only student information that is necessary
- Limit access to student files
- Train employees to recognize security threats
- Report and log all suspected identity theft incidents
- Incorporate disciplinary procedures for employees who do not comply with above mentioned procedures

Updating the Program

The institution will update the program periodically to reflect changes in risk to student's or in reference to the safety and soundness of the organization.

Factors that will require a review or update of our procedure will include the following:

- Experiences of the organization with identity theft
- New methods of committing identity theft
- Improvements made in the methods used to detect, prevent and mitigate identity theft
- Changes in the types of accounts that the organization offers
- Changes in the business arrangements of the organization
- The introduction of new service providers

Administration of the Program

The Director of the School shall be responsible for the development.

Safeguarding Customer Information

July 1, 2011

The Program will train staff, as necessary, to effectively implement the Program and the Program shall exercise appropriate and effective "oversight" procedures.

Oversight of the Program

- Review of reports prepared by the staff regarding compliance
- Approval of material changes to the Program as necessary to address changing risks of identity theft
- Analysis of the effectiveness of policies and procedures
- Service provider agreements
- Actual detection of "red flags" and the action taken
- Recommendations for changes to the Program